UNITED STATES DISTRICT COURT

WESTERN DISTRICT OF WASHINGTON

SEATTLE DIVISION

KEYONNA DANIELS, on behalf of herself and all others similarly situated, Plaintiff, v. LABORATORY SERVICES COOPERATIVE, Defendant.	Case No. 2:25-cv-685 **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

Plaintiff, Keyonna Daniels ("Plaintiff"), on behalf of herself and all others similarly situated, states as follows for her class action complaint against Defendant, Laboratory Services Cooperative ("LSC" or "Defendant"):

INTRODUCTION

1. This Class Action arises from a recent cyberattack resulting in a data breach of sensitive information in the possession and custody and/or control of Defendant (the "Data Breach").

2. On information and belief, the Data Breach was discovered by Defendant on October 27, 2024. Following an internal investigation, Defendant learned the Data Breach resulted in the unauthorized disclosure, exfiltration, and theft of its clients' current and former patients'

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

highly personal information, including Social Security Number, driver's license or state ID number, passport number, date of birth, demographic data, student ID number, and other forms of government identifiers, insurance information, banking and financial information, ("personally identifying information" or "PII"), diagnosis, treatment, medical record number, lab results, patient number, provider name, treatment location, and related care details ("protected health information" or "PHI"). Plaintiff refers to both PII and PHI collectively as "Sensitive Information."

3. LSC's breach differs from typical data breaches because it affects patients who had no relationship with LSC, never sought one, and never consented to LSC collecting and storing their information.

4. LSC sourced their information from third parties, including Planned Parenthood, stored it on LSC's systems, and assumed a duty to protect it. However LSC never implemented the security safeguards needed despite understanding its importance.

5. On or around April 10, 2025–six months after the Data Breach was first discovered–LSC finally began notifying Class Members about the Data Breach ("Breach Notice"). The Breach Notice is attached as Exhibit A. However, notice is ongoing, with many Class Members, including Plaintiff, still awaiting their formal notice.

6. Due to intentionally obfuscating language, it is unclear when the Breach actually took place and how long cybercriminals had unfettered access to Plaintiff's and the Class's most sensitive information.

7. LSC took at least six months before informing some Class Members even though Plaintiff and thousands of Class Members had their most sensitive personal information accessed, exfiltrated, and stolen, causing them to suffer ascertainable losses in the form of the loss of the benefit of their bargain and the value of their time reasonably incurred to remedy or mitigate the effects of the attack.

8. LSC's Breach Notice obfuscated the nature of the breach and the threat it posted—refusing to tell its patients when the Breach occurred, how many people were impacted, how the

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

breach happened, and why it took Defendant until April 2025 to begin notifying victims that hackers had gained access to highly private Sensitive Information.

9. Defendant's failure to timely detect and report the Data Breach made its patients vulnerable to identity theft without any warnings to monitor their financial accounts or credit reports to prevent unauthorized use of their Sensitive Information.

10. Defendant knew or should have known that each victim of the Data Breach deserved prompt and efficient notice of the Data Breach and assistance in mitigating the effects of PII and PHI misuse.

11. In failing to adequately protect Plaintiff's and the Class's Sensitive Information, failing to adequately notify them about the breach, and by obfuscating the nature of the breach, Defendant violated state and federal law and harmed an unknown number of its current and former patients and prospective patients.

12. Plaintiff and members of the proposed Class are victims of Defendant's negligence and inadequate cyber security measures. Specifically, Plaintiff and members of the proposed Class trusted Defendant with their Sensitive Information. But Defendant betrayed that trust. Defendant failed to properly use up-to-date security practices to prevent the Data Breach.

13. Plaintiff is a current patient of Planned Parenthood, which LSC provides its lab testing services to.

14. Accordingly, Plaintiff, on behalf of herself and a class of similarly situated individuals, brings this lawsuit seeking injunctive relief, damages, and restitution, together with costs and reasonable attorneys' fees, the calculation of which will be based on information in Defendant's possession.

PARTIES

15. Plaintiff, Keyonna Daniels is a natural person and citizen of Sacramento, California, where she intends to remain.

16. Defendant, Laboratory Services Cooperative, is a Washington corporation, with its principal place of business at 2001 E Madison Street, Seattle, Washington, 98122-2959.

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

JURISDICTION AND VENUE

17. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. Plaintiff and Defendant are of different states. And there are over 100 putative Class members.

18. This Court has personal jurisdiction over Defendant because it is headquartered in Washington, regularly conducts business in Washington, and has sufficient minimum contacts in Washington.

19. Venue is proper in this Court because Defendant's principal office is in this District, and because a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District.

STATEMENT OF FACTS

LSC

20. LSC is a Washington state-based diagnostic testing services provider."[1] Defendant boasts a total annual revenue between $18 million.[2]

21. As part of its business, Defendant receives and maintains the Sensitive Information of thousands of patients (such as, *inter alia*, its clients' patients). In collecting and maintaining Sensitive Information, Defendant agreed it would safeguard the data in accordance with its internal policies, state law, and federal law. After all, Plaintiff and Class members themselves took reasonable steps to secure their Sensitive Information.

22. Despite recognizing its duty to do so, on information and belief, LSC has not implemented reasonable cybersecurity safeguards or policies to protect its patients' Sensitive Information or supervised its IT or data security agents and employees to prevent, detect, and stop

[1] SC Media, https://www.scworld.com/brief/attack-against-laboratory-services-cooperative-impacts-1-6m (last visited April 16, 2025).
[2]ProPublica, = https://projects.propublica.org/nonprofits/organizations/263813271 (last visited April 16, 2025).

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

breaches of its systems. As a result, LSC leaves significant vulnerabilities in its systems for cybercriminals to exploit and gain access to patients' Sensitive Information.

The Data Breach

23. Plaintiff is unsure how LSC got her information but assumes that Planned Parenthood, where she receives medical services, provided LSC with her Sensitive Information.

24. On information and belief, Defendant collects and maintains patients' Sensitive Information in its computer systems.

25. In collecting and maintaining Sensitive Information, Defendant implicitly agrees that it will safeguard the data using reasonable means according to state and federal law.

26. According to its Breach Notice, on October 27, 2024, Defendant was alerted that "LSC identified suspicious activity within its network." Ex. A. Following an internal investigation, Defendant confirmed that "certain LSC patient and worker-related data" had been affected by the unauthorized actor. *Id*.

27. In other words, Defendant's cyber and data security systems were so completely inadequate that it allowed cybercriminals to obtain files containing a treasure trove of thousands of its patients' highly private Sensitive Information.

28. Through its inadequate security practices, Defendant exposed Plaintiff's and the Class's Sensitive Information for theft and sale on the dark web.

29. On or around April 10, 2025—six months after the Breach was discovered— LSC finally began notifying Class Members about the Data Breach. However, notification is ongoing with many Class Members, including Plaintiff still awaiting formal notice.

30. Despite its duties and alleged commitments to safeguard Sensitive Information, Defendant did not in fact follow industry standard practices in securing patients' Sensitive Information, as evidenced by the Data Breach.

31. Typically in response to the Data Breach, a company will promise to implement enhancement and additional cybersecurity steps to prevent a similar breach from occurring again. Not Defendant. Instead, Defendant places the onus on Plaintiff and the Class, informing them to

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

regularly review their accounts and credit reports for instances of fraud and identity theft caused by Defendant's inadequate cybersecurity.

32. Through its Breach Notice, Defendant also recognized the actual imminent harm and injury that flowed from the Data Breach, so it encouraged breach victims to be "vigilant by regularly reviewing your accounts and monitoring credit reports for suspicious activity." Ex. A.

33. Defendant further recognize its duty to provide adequate cybersecurity, insisting that, despite the Breach demonstrating otherwise "The confidentiality, privacy, and security of information maintained by LSC remains its top priority." Ex. A.

34. Cybercriminals need not harvest a person's Social Security number or financial account information in order to commit identity fraud or misuse Plaintiff's and the Class's Sensitive Information. Cybercriminals can cross-reference the data stolen from the Data Breach and combine with other sources to create "Fullz" packages, which can then be used to commit fraudulent account activity on Plaintiff's and the Class's financial accounts.

35. On information and belief, LSC has offered several months of complimentary credit monitoring services to victims, which does not adequately address the lifelong harm that victims will face following the Data Breach. Indeed, the breach involves Sensitive Information that cannot be changed, such as Social Security numbers.

36. Even with several months' worth of credit monitoring services, the risk of identity theft and unauthorized use of Plaintiff's and Class Members' Sensitive Information is still substantially high. The fraudulent activity resulting from the Data Breach may not come to light for years.

37. On information and belief, Defendant failed to adequately train and supervise its IT and data security agents and employees on reasonable cybersecurity protocols or implement reasonable security measures, causing it to lose control over its patients' Sensitive Information. Defendant's negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing the Sensitive Information.

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

The Data Breach was a Foreseeable Risk of which Defendant was on Notice.

38. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the healthcare and healthcare adjacent industry preceding the date of the breach.

39. In light of recent high profile data breaches at other healthcare and healthcare adjacent companies, Defendant knew or should have known that its electronic records and patients' Sensitive Information would be targeted by cybercriminals.

40. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[3] The 330 reported breaches reported in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.[4]

41. Indeed, cyberattacks against the healthcare industry have become increasingly common for over ten years, with the FBI warning as early as 2011 that cybercriminals were "advancing their abilities to attack a system remotely" and "[o]nce a system is compromised, cyber criminals will use their accesses to obtain PII." The FBI further warned that that "the increasing sophistication of cyber criminals will no doubt lead to an escalation in cybercrime." [5]

42. Cyberattacks on medical systems and healthcare and healthcare adjacent companies like Defendant have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive. . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[6]

---

[3] 2021 Data Breach Annual Report, ITRC, chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.wsav.com/wp-content/uploads/sites/75/2022/01/20220124_ITRC-2021-Data-Breach-Report.pdf (last visited January 10, 2024).

[4] *Id.*

[5] Gordon M. Snow Statement, FBI https://archives.fbi.gov/archives/news/testimony/cyber-security-threats-to-the-financial-sector (last visited January 10, 2024).

[6] Secret Service Warn of Targeted, Law360, https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware (last visited January 10, 2024).

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

43. In fact, many high-profile ransomware attacks have occurred in healthcare and healthcare adjacent companies, with an estimated that nearly half of all ransomware attacks being carried out are on healthcare companies, and with 85% of those attacks being ransomware similar to the one occurring here.[7]

44. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including Defendant.

Plaintiff's Experience

45. Plaintiff is unsure how LSC got her information but assumes that Planned Parenthood, where she receives medical services, provided LSC with her Sensitive Information.

46. Regardless, Defendant obtained and continues to maintain Plaintiff's Sensitive Information. Defendant has a continuing legal duty and obligation to protect that Sensitive Information from unauthorized access and disclosure.

47. Defendant deprived Plaintiff of the earliest opportunity to guard herself against the Data Breach's effects by delaying notification of the Breach.

48. As a result of its inadequate cybersecurity, Defendant exposed Plaintiff's Sensitive Information for theft by cybercriminals and sale on the dark web.

49. As a result of the Data Breach notice, Plaintiff spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach, self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred. This time has been lost forever and cannot be recaptured.

50. Plaintiff has and will spend considerable time and effort monitoring her accounts to protect herself from additional identity theft. Plaintiff fears for her personal financial security and uncertainty over what Sensitive Information was exposed in the Data Breach.

51. Plaintiff has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or

[7] Ransomware explained, CSO, https://www.csoonline.com/article/563507/what-is-ransomware-how-it-works-and-how-to-remove-it.html (last visited January 10, 2024);

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

52. Plaintiff has suffered actual injury in the form of damages to and diminution in the value of their Sensitive Information—a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and as a result of the Data Breach.

53. Plaintiff suffered actual injury from the exposure of her Sensitive Information — which violates her rights to privacy.

54. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her Sensitive Information being placed in the hands of unauthorized third parties and possibly criminals.

55. Indeed, shortly after the Data Breach, Plaintiff began suffering a significant increase in spam calls and emails. These spam calls suggest that her Sensitive Information is now in the hands of cybercriminals.

56. Once an individual's PII is for sale and access on the dark web, as Plaintiff's PII is here as a result of the Breach, cybercriminals are able to use the stolen and compromised to gather and steal even more information.[8] On information and belief, Plaintiff's phone number and email address were compromised as a result of the Data Breach.

57. Plaintiff has a continuing interest in ensuring that her Sensitive Information, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

Plaintiff and the Proposed Class Face Significant Risk of Continued Identity Theft

58. Plaintiff and members of the proposed Class have suffered injury from the misuse of their Sensitive Information that can be directly traced to Defendant.

[8] What do Hackers do with Stolen Information, Aura, https://www.aura.com/learn/what-do-hackers-do-with-stolen-information (last visited January 9, 2024).

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

59. As a result of Defendant's failure to prevent the Data Breach, Plaintiff and the proposed Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

a. The loss of the opportunity to control how their Sensitive Information is used;

b. The diminution in value of their Sensitive Information;

c. The compromise and continuing publication of their Sensitive Information;

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen Sensitive Information; and

h. The continued risk to their Sensitive Information, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake the appropriate measures to protect the Sensitive Information in its possession.

60. Stolen Sensitive Information is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII alone can be worth up to $1,000.00 depending on the type of information obtained.

61. The value of Plaintiff's and the Class's Sensitive Information on the black market is considerable. Stolen Sensitive Information trades on the black market for years, and criminals frequently post stolen Sensitive Information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

62. It can take victims years to spot identity theft, giving criminals plenty of time to use that information for cash.

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

63. One such example of criminals using Sensitive Information for profit is the development of "Fullz" packages.

64. Cyber-criminals can cross-reference two sources of Sensitive Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

65. The development of "Fullz" packages means that stolen Sensitive Information from the Data Breach can easily be used to link and identify it to Plaintiff and the proposed Class' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Sensitive Information stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff's and the Class's stolen Sensitive Information is being misused, and that such misuse is fairly traceable to the Data Breach.

66. Defendant disclosed the Sensitive Information of Plaintiff and the Class for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the Sensitive Information of Plaintiff and the Class to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen Sensitive Information.

67. Defendant's failure to properly notify Plaintiff and members of the Class of the Data Breach exacerbated Plaintiff's and the Class's injury by depriving them of the earliest ability to take appropriate measures to protect their Sensitive Information and take other necessary steps to mitigate the harm caused by the Data Breach.

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

Defendant failed to adhere to FTC guidelines.

68. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as Defendant, should employ to protect against the unlawful exposure of Sensitive Information.

69. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business. The guidelines explain that businesses should:

a. protect the sensitive consumer information that it keeps;

b. properly dispose of Sensitive Information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

70. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

71. The FTC recommends that companies not maintain information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

72. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

73. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to consumers' Sensitive Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Defendant Violated HIPAA

74. HIPAA circumscribes security provisions and data privacy responsibilities designed to keep patients' medical information safe. HIPAA compliance provisions, commonly known as the Administrative Simplification Rules, establish national standards for electronic transactions and code sets to maintain the privacy and security of protected health information. [9]

75. HIPAA provides specific privacy rules that require comprehensive administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of PII and PHI is properly maintained.[10]

76. The Data Breach itself resulted from a combination of inadequacies showing Defendant's failure to comply with safeguards mandated by HIPAA. Defendant's security failures include, but are not limited to:

a. Failing to ensure the confidentiality and integrity of electronic PHI that it creates, receives, maintains and transmits in violation of 45 C.F.R. § 164.306(a)(1);

b. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

c. Failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

---

[9] HIPAA lists 18 types of information that qualify as PHI according to guidance from the Department of Health and Human Services Office for Civil Rights, and includes, inter alia: names, addresses, any dates including dates of birth, Social Security numbers, and medical record numbers.

[10] *See* 45 C.F.R. § 164.306 (security standards and general rules); 45 C.F.R. § 164.308 (administrative safeguards); 45 C.F.R. § 164.310 (physical safeguards); 45 C.F.R. § 164.312 (technical safeguards).

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

d. Failing to ensure compliance with HIPAA security standards by Defendant in violation of 45 C.F.R. § 164.306(a)(4);

e. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

f. Failing to implement policies and procedures to prevent, detect, contain and correct security violations in violation of 45 C.F.R. § 164.308(a)(1);

g. Failing to identify and respond to suspected or known security incidents and failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii);

h. Failing to effectively train all staff members on the policies and procedures with respect to PHI as necessary and appropriate for staff members to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5); and

i. Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI, in compliance with 45 C.F.R. § 164.530(c).

77. Simply put, the Data Breach resulted from a combination of insufficiencies that demonstrate Defendant failed to comply with safeguards mandated by HIPAA regulations.

Consumers Prioritize Data Security

78. In 2024, the technology and communications conglomerate Cisco published the results of its multi-year "Consumer Privacy Survey."[11] Therein, Cisco reported the following:

[11] *Privacy Awareness: Consumers Taking Charge to Protect Personal*, CISCO, https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-consumer-privacy-report-2024.pdf (last visited March 19, 2025).

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

a. "For the past six years, Cisco has been tracking consumer trends across the privacy landscape. During this period, privacy has evolved from relative obscurity to a customer requirement with more than 75% of consumer respondents saying they won't purchase from an organization they don't trust with their data."[12]

b. "Privacy has become a critical element and enabler of customer trust, with 94% of organizations saying their customers would not buy from them if they did not protect data properly."[13]

c. 89% of consumers stated that "I care about data privacy."[14]

d. 83% of consumers declared that "I am willing to spend time and money to protect data" and that "I expect to pay more" for privacy.[15]

e. 51% of consumers revealed that "I have switched companies or providers over their data policies or data-sharing practices."[16]

f. 75% of consumers stated that "I will not purchase from organizations I don't trust with my data."[17]

79. Defendant knew or should have known that adequate implementation of cybersecurity and protection of Sensitive Information, including Plaintiff and the Class's Sensitive Information was important to its client's patients.

Defendant Fails to Comply with Industry Standards

80. As noted above, experts studying cyber security routinely identify entities in possession of PII and PHI as being particularly vulnerable to cyberattacks because of the value of the Sensitive Information which they collect and maintain.

81. Several best practices have been identified that a minimum should be implemented by employers in possession of PII and PHI, like Defendant, including but not limited to: educating

[12] *Id*. at 3.
[13] *Id*.
[14] *Id*. at 9.
[15] *Id*.
[16] *Id*.
[17] *Id*. at 11.

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which employees can access sensitive data. Defendant failed to follow these industry best practices, including a failure to implement multi-factor authentication.

82. Other best cybersecurity practices that are standard for employers include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points. Defendant failed to follow these cybersecurity best practices, including failure to train staff.

83. Upon information and belief, Defendants failed to implement industry-standard cybersecurity measures, including failing to meet the minimum standards of both the NIST Cybersecurity Framework Version 2.0 (including without limitation PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04).

84. These foregoing frameworks are existing and applicable industry standards for an employer's obligations to provide adequate data security for its employees. Upon information and belief, Defendant failed to comply with at least one—or all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

CLASS ACTION ALLEGATIONS

85. Plaintiff is suing on behalf of herself and the proposed Class ("Class"), defined as follows:

> All US citizens whose Sensitive Information was compromised in the Data Breach discovered by Defendant in June 2024, including all those citizens who received notice of the breach.

86. Excluded from the Class is Defendant, their agents, affiliates, parents, subsidiaries, any entity in which Defendant have a controlling interest, any of Defendant's officers or directors,

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

any successors, and any Judge who adjudicates this case, including their staff and immediate family.

87. Plaintiff reserves the right to amend the class definition.

a. **Numerosity**. Plaintiff is representative of the Class, consisting of several thousands of members, far too many to join in a single action;

b. **Ascertainability**. Members of the Class are readily identifiable from information in Defendant's possession, custody, and control;

c. **Typicality**. Plaintiff's claims are typical of class claims as each arises from the same Data Breach, the same alleged violations by Defendant, and the same unreasonable manner of notifying individuals about the Data Breach.

d. **Adequacy**. Plaintiff will fairly and adequately protect the proposed Class's interests. Her interests do not conflict with the Class's interests, and she has retained counsel experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf, including as lead counsel.

e. **Commonality**. Plaintiff's and the Class's claims raise predominantly common fact and legal questions that a class wide proceeding can answer for the Class. Indeed, it will be necessary to answer the following questions:

i. Whether Defendant had a duty to use reasonable care in safeguarding Plaintiff's and the Class's Sensitive Information;

ii. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

iii. Whether Defendant were negligent in maintaining, protecting, and securing Sensitive Information;

iv. Whether Defendant breached contract promises to safeguard Plaintiff's and the Class's Sensitive Information;

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

v. Whether Defendant took reasonable measures to determine the extent of the Data Breach after discovering it;

vi. Whether Defendant's Breach Notice was reasonable;

vii. Whether the Data Breach caused Plaintiff's and the Class's injuries;

viii. What the proper damages measure is; and

ix. Whether Plaintiff and the Class are entitled to damages, treble damages, or injunctive relief.

88. Further, common questions of law and fact predominate over any individualized questions, and a class action is superior to individual litigation or any other available method to fairly and efficiently adjudicate the controversy. The damages available to individual plaintiffs are insufficient to make individual lawsuits economically feasible.

COUNT I
Negligence
(On Behalf of Plaintiff and the Class)

89. Plaintiff realleges all previous paragraphs as if fully set forth below.

90. Plaintiff and the Class entrusted their Sensitive Information to Defendant on the premise and with the understanding that Defendant would safeguard their Sensitive Information, use their Sensitive Information for business purposes only, and/or not disclose their Sensitive Information to unauthorized third parties.

91. Defendant owed a duty of care to Plaintiff and Class members because it was foreseeable that Defendant's failure—to use adequate data security in accordance with industry standards for data security—would compromise their Sensitive Information in a data breach. And here, that foreseeable danger came to pass.

92. Defendant has full knowledge of the sensitivity of the Sensitive Information and the types of harm that Plaintiff and the Class could and would suffer if their Sensitive Information was wrongfully disclosed.

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

93. Defendant owed these duties to Plaintiff and Class members because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security practices. After all, Defendant actively sought and obtained Plaintiff's and Class members' Sensitive Information.

94. Defendant owed—to Plaintiff and Class members—at least the following duties to:

a. exercise reasonable care in handling and using the Sensitive Information in its care and custody;

b. implement industry-standard security procedures sufficient to reasonably protect the information from a data breach, theft, and unauthorized;

c. promptly detect attempts at unauthorized access;

d. notify Plaintiff and Class members within a reasonable timeframe of any breach to the security of their Sensitive Information.

95. Thus, Defendant owed a duty to timely and accurately disclose to Plaintiff and Class members the scope, nature, and occurrence of the Data Breach. After all, this duty is required and necessary for Plaintiff and Class members to take appropriate measures to protect their Sensitive Information, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

96. Defendant also had a duty to exercise appropriate clearinghouse practices to remove Sensitive Information it was no longer required to retain under applicable regulations.

97. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the Sensitive Information of Plaintiff and the Class involved an unreasonable risk of harm to Plaintiff and the Class, even if the harm occurred through the criminal acts of a third party.

98. Defendant's duty to use reasonable security measures arose because of the special relationship that existed between Defendant and Plaintiff and the Class. That special relationship

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

arose because Plaintiff's and the Class entrusted Defendant with their confidential Sensitive Information, a necessary part of obtaining services from Defendant.

99. Under the FTC Act, 15 U.S.C. § 45, Defendant had a duty to use fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class members' Sensitive Information.

100. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect the Sensitive Information entrusted to it. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiff's and the Class members' sensitive Information.

101. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect Sensitive Information and not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of Sensitive Information Defendant had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

102. Similarly, under HIPAA, Defendant had a duty to follow HIPAA standards for privacy and security practices—as to protect Plaintiff's and Class members' PHI.

103. Defendant violated its duty under HIPAA by failing to use reasonable measures to protect its PHI and by not complying with applicable regulations detailed supra. Here too, Defendant's conduct was particularly unreasonable given the nature and amount of PHI that Defendant collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

104. The risk that unauthorized persons would attempt to gain access to the Sensitive Information and misuse it was foreseeable. Given that Defendant hold vast amounts of Sensitive

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

Information, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the Sensitive Information —whether by malware or otherwise.

105. Sensitive Information is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the Sensitive Information of Plaintiff and Class members and the importance of exercising reasonable care in handling it.

106. Defendant improperly and inadequately safeguarded the Sensitive Information of Plaintiff and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

107. Defendant breached these duties as evidenced by the Data Breach.

108. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiff's and Class members' Sensitive Information by:

a. disclosing and providing access to this information to third parties and

b. failing to properly supervise both the way the Sensitive Information was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

109. Defendant breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the personal information and Sensitive Information of Plaintiff and Class members which actually and proximately caused the Data Breach and Plaintiff's and Class members' injury.

110. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiff and Class members, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiff's and Class members' injuries-in-fact.

111. Defendant has admitted that the Sensitive Information of Plaintiff and the Class was wrongfully lost and disclosed to unauthorized third persons because of the Data Breach.

112. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiff and Class members have suffered or will suffer damages, including monetary

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

113. And, on information and belief, Plaintiff's Sensitive Information has already been published—or will be published imminently—by cybercriminals on the dark web.

114. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiff and Class members actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their Sensitive Information by criminals, improper disclosure of their Sensitive Information, lost benefit of their bargain, lost value of their Sensitive Information, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

COUNT II
Breach of Contract
(On Behalf of Plaintiff and the Class)

115. Plaintiff realleges all previous paragraphs as if fully set forth below.

116. Defendant entered into various contracts with its clients, to provide laboratory services to its clients.

117. These contracts are virtually identical to each other and were made expressly for the benefit of Plaintiff and the Class, as it was their confidential information that Defendant agreed to collect and protect through its services. Thus, the benefit of collection and protection of the Sensitive Information belonging to Plaintiff and the Class were the direct and primary objective of the contracting parties.

118. Defendant knew that if it were to breach these contracts with its clients, the clients' consumers, including Plaintiff and the Class, would be harmed by, among other things, fraudulent misuse of their Sensitive Information.

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

119. Defendant breached its contracts with its clients when it failed to use reasonable data security measures that could have prevented the Data Breach and resulting compromise of Plaintiff's and Class Members' Sensitive Information.

120. As reasonably foreseeable result of the breach, Plaintiff and the Class were harmed by Defendant failure to use reasonable data security measures to store their Sensitive Information, including but not limited to, the actual harm through the loss of their Sensitive Information to cybercriminals.

121. Accordingly, Plaintiff and the Class are entitled to damages in an amount to be determined at trial, along with their costs and attorney fees incurred in this action.

COUNT III
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

122. Plaintiff realleges all previous paragraphs as if fully set forth below.

123. This claim is pleaded in the alternative to the breach of contractual duty claim.

124. Plaintiff and members of the Class (or their third-party agents) conferred a benefit upon Defendant in providing Sensitive Information to Defendant.

125. Defendant appreciated or had knowledge of the benefits conferred upon it by Plaintiff and the Class. Defendant also benefited from the receipt of Plaintiff's and the Class's Sensitive Information, as this was used to facilitate the services and goods it sold to Plaintiff and the Class.

126. Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiff and the Class's Sensitive Information because Defendant failed to adequately protect their Sensitive Information. Plaintiff and the proposed Class would not have provided their Sensitive Information to Defendant had they known Defendant would not adequately protect their Sensitive Information.

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

127. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and members of the Class all unlawful or inequitable proceeds received by them because of their misconduct and Data Breach.

COUNT IV
Invasion of Privacy
(On Behalf of Plaintiff and the Class)

128. Plaintiff realleges all previous paragraphs as if fully set forth below.

129. Plaintiff and the Class had a legitimate expectation of privacy regarding their highly confidential Sensitive Information and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

130. Defendant owed a duty to its client's current and former patients, including Plaintiff and the Class, to keep this information confidential.

131. The unauthorized acquisition (i.e., theft) by a third party of Plaintiff's and Class members' Sensitive Information is highly offensive to a reasonable person.

132. The intrusion was into a place or thing which was private and entitled to be private. Plaintiff and the Class disclosed their sensitive and confidential information to Defendant, but did so privately, with the intention that their information would be kept confidential and protected from unauthorized disclosure. Plaintiff and the Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

133. The Data Breach constitutes an intentional interference with Plaintiff's and the Class's interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

134. Defendant acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

135. Defendant acted with a knowing state of mind when it failed to notify Plaintiff and the Class in a timely fashion about the Data Breach, thereby materially impairing their mitigation efforts.

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

136. Acting with knowledge, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiff and the Class.

137. As a proximate result of Defendant's acts and omissions, the private Sensitive Information of Plaintiff and the Class were stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiff and the Class to suffer damages (as detailed *supra*).

138. And, on information and belief, Plaintiff's Sensitive Information has already been published—or will be published imminently—by cybercriminals on the dark web.

139. Unless and until enjoined and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class since their Sensitive Information are still maintained by Defendant with their inadequate cybersecurity system and policies.

140. Plaintiff and the Class have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendant's inability to safeguard the Sensitive Information of Plaintiff and the Class.

141. In addition to injunctive relief, Plaintiff, on behalf of herself and the other Class members, also seek compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest and costs.

COUNT V
Violation of the Washington Consumer Protection Act RCW 19.86
(On Behalf of Plaintiff and the Class)

142. Plaintiff realleges all previous paragraphs as if fully set forth below.

148. The Washington State Consumer Protection Act, RCW 19.86.020 (the "CPA") prohibits any "unfair or deceptive acts or practices" in the conduct of any trade or commerce as those terms are described by the CPA and relevant case law.

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

149. Defendant is a "person" as described in RCW 19.86.010(1).

150. Defendant engages in "trade" and "commerce" as described in RCW 19.86.010(2) in that it engages in the sale of services and commerce directly and indirectly affecting the people of the state of Washington.

151. By virtue of the above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, Defendant engaged in unlawful, unfair, and fraudulent practices within the meaning of, and in violation of, the CPA, in that Defendant's practices were injurious to the public interest because they injured other persons, had the capacity to injure other persons, and have the capacity to injure other persons.

152. Defendant's failure to safeguard the Sensitive Information exposed in the Data Breach constitutes an unfair act that offends public policy.

153. Defendant's failure to safeguard the Sensitive Information compromised in the Data Breach caused substantial injury to Plaintiff's and Class Members. Defendant's failure is not outweighed by any countervailing benefits to consumers or competitors, and it was not reasonably avoidable by consumers.

154. Defendant's failure to safeguard the Sensitive Information disclosed in the Data Breach, and its failure to provide timely and complete notice of that Data Breach to the victims, is unfair because these acts and practices are immoral, unethical, oppressive, and/or unscrupulous.

155. In the course of conducting its business, Defendant committed "unfair or deceptive acts or practices" by, *inter alia*, knowingly failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiff's and Class Members' Sensitive Information, and violating the common law alleged herein in the process. Plaintiff and Class Members reserve the right to allege other violations of law by Defendant constituting other unlawful business acts or practices. As described above,

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

Defendant's wrongful actions, inaction, omissions, and want of ordinary care are ongoing and continue to this date.

156. Defendant also violated the CPA by failing to timely notify, and by concealing from Plaintiff and Class Members, information regarding the unauthorized release and disclosure of their Sensitive Information. If Plaintiff and Class Members had been notified in an appropriate fashion, and had the information not been hidden from them, they could have taken precautions to safeguard and protect their Sensitive Information.

157. The gravity of Defendant's wrongful conduct outweighs any alleged benefits attributable to such conduct. There were reasonably available alternatives to further Defendant's legitimate business interests other than engaging in the above-described wrongful conduct.

158. Defendant's unfair or deceptive acts or practices occurred in its trade or business and have injured and are capable of injuring a substantial portion of the public. Defendant's general course of conduct as alleged herein is injurious to the public interest, and the acts complained of herein are ongoing and/or have a substantial likelihood of being repeated.

159. As a direct and proximate result of Defendant's above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach and its violations of the CPA, Plaintiff and Class Members have suffered, and will continue to suffer, economic damages and other injury and actual harm in the form of, *inter alia*, (i) an imminent, immediate, and continuing increased risk of identity theft and identity fraud—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) invasion of privacy; (iii) breach of the confidentiality of their PII; (iv) deprivation of the value of their PII, for which there is a well-established national and international market; and/or (v) the financial and temporal costs of monitoring credit, monitoring financial accounts, and mitigating damages.

160. Unless restrained and enjoined, Defendant will continue to engage in the above-described wrongful conduct and more data breaches will occur. Plaintiff, therefore, on behalf of themselves and the Class, seek restitution and an injunction prohibiting Defendant from

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

continuing such wrongful conduct, and requiring Defendant to design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures protocols, and software and hardware systems to safeguard and protect the Sensitive Information entrusted to it.

161. Plaintiff, on behalf of herself and Class Members, also seek to recover actual damages sustained by each Class Member together with the costs of the suit, including reasonable attorneys' fees. In addition, Plaintiff, on behalf of herself and Class Members, request that this Court use its discretion, pursuant to RCW 19.86.090, to increase the damages award for each Class Member by three times the actual damages sustained, not to exceed $25,000.00 per Class Member.

COUNT VI
Violation of the California Customer Records Act
Cal. Civ. Code § 1798.80, et seq.
(On Behalf of Plaintiff and the Class)

162. Plaintiff realleges all previous paragraphs as if fully set forth below.

163. Under the California Customer Records Act, any "person or business that conducts business in California, and that owns or licenses computerized data that includes personal information" must "disclose any breach of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Cal. Civ. Code § 1798.82. The disclosure must "be made in the most expedient time possible and without unreasonable delay" but disclosure must occur "immediately following discovery [of the breach], if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person." *Id* (emphasis added).

164. The Data Breach constitutes a "breach of the security system" of Defendant.

165. An unauthorized person acquired the personal, unencrypted information of Plaintiff and the Class.

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

166. Defendant knew that an unauthorized person had acquired the personal, unencrypted information of Plaintiff and the Class but waited approximately two months to notify them. Given the severity of the Data Breach, six months was an unreasonable delay.

167. Defendant's unreasonable delay prevented Plaintiff and the Class from taking appropriate measures from protecting themselves against harm.

168. Because Plaintiff and the Class were unable to protect themselves, they suffered incrementally increased damages that they would not have suffered with timelier notice.

169. Plaintiff and the Class are entitled to equitable relief and damages in an amount to be determined at trial.

COUNT VII
Violation of California's Unfair Competition Law ("UCL")
Cal Bus. & Prof. Code § 17200, *et seq.*
(On Behalf of Plaintiff and the Class)

170. Plaintiff realleges all previous paragraphs as if fully set forth below.

171. Defendant engaged in unlawful and unfair business practices in violation of Cal. Bus. & Prof. Code § 17200, *et seq*. which prohibits unlawful, unfair, or fraudulent business acts or practices ("UCL").

172. Defendant's conduct is unlawful because it violates the California Consumer Privacy Act of 2018, Civ. Code § 1798.100, *et seq*. (the "CCPA"), and other state data security laws.

173. Defendant stored the Sensitive Information of Plaintiff and the Class in its computer systems and knew or should have known it did not employ reasonable, industry standard, and appropriate security measures that complied with applicable regulations and that would have kept Plaintiff's and the Class's Sensitive Information secure so as to prevent the loss or misuse of that Sensitive Information.

174. Defendant failed to disclose to Plaintiff and the Class that their Sensitive Information was not secure. However, Plaintiff and the Class were entitled to assume, and did assume, that Defendant had secured their Sensitive Information. At no time were Plaintiff and

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

the Class on notice that their Sensitive Information was not secure, which Defendant had a duty to disclose.

175. Defendant also violated California Civil Code § 1798.150 by failing to implement and maintain reasonable security procedures and practices, resulting in an unauthorized access and exfiltration, theft, or disclosure of Plaintiff's and the Class's nonencrypted and nonredacted Sensitive Information.

176. Had Defendant complied with these requirements, Plaintiff and the Class would not have suffered the damages related to the data breach.

177. Defendant's acts, omissions, and misrepresentations as alleged herein were unlawful and in violation of, *inter alia*, Section 5(a) of the Federal Trade Commission Act.

178. Defendant's conduct was also unfair, in that it violated a clear legislative policy in favor of protecting consumers from data breaches.

179. Defendant's conduct is an unfair business practice under the UCL because it was immoral, unethical, oppressive, and unscrupulous and caused substantial harm. This conduct includes employing unreasonable and inadequate data security despite its business model of actively collecting Sensitive Information.

180. Defendant also engaged in unfair business practices under the "tethering test." Its actions and omissions, as described above, violated fundamental public policies expressed by the California Legislature. *See, e.g.,* Cal. Civ. Code § 1798.1 ("The Legislature declares that . . . all individuals have a right of privacy in information pertaining to them . . . The increasing use of computers . . . has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information."); Cal. Civ. Code § 1798.81.5(a) ("It is the intent of the Legislature to ensure that personal information about California residents is protected."); Cal. Bus. & Prof. Code § 22578 ("It is the intent of the Legislature that this chapter [including the Online Privacy Protection Act] is a matter of statewide concern."). Defendant's acts and omissions thus amount to a violation of the law.

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

181. Instead, Defendant made the Sensitive Information of Plaintiff and the Class accessible to scammers, identity thieves, and other malicious actors, subjecting Plaintiff and the Class to an impending risk of identity theft. Additionally, Defendant's conduct was unfair under the UCL because it violated the policies underlying the laws set out in the prior paragraph.

182. As a result of those unlawful and unfair business practices, Plaintiff and the Class suffered an injury-in-fact and have lost money or property.

183. The injuries to Plaintiff and the Class greatly outweigh any alleged countervailing benefit to consumers or competition under all of the circumstances.

184. There were reasonably available alternatives to further Defendant's legitimate business interests, other than the misconduct alleged in this complaint.

185. Therefore, Plaintiff and the Class are entitled to equitable relief, including restitution of all monies paid to or received by Defendant; disgorgement of all profits accruing to Defendant because of its unfair and improper business practices; a permanent injunction enjoining Defendant's unlawful and unfair business activities; and any other equitable relief the Court deems proper.

COUNT VIII
Violation of California's Unfair Competition Law ("UCL")
Cal Bus. & Prof. Code § 17200, *et seq.*
(On Behalf of Plaintiff and the Class)

186. Plaintiff realleges all previous paragraphs as if fully set forth below.

187. Defendant violated California Civil Code § 1798.150 of the CCPA by failing to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the nonencrypted Sensitive Information of Plaintiff and the Class. As a direct and proximate result, Plaintiff's, and the Class's nonencrypted and nonredacted Sensitive Information was subject to unauthorized access and exfiltration, theft, or disclosure.

188. Defendant is a business organized for the profit and financial benefit of its owners according to California Civil Code § 1798.140, that collects the personal information of its

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

customers, and whose annual gross revenues exceed the threshold established by California Civil Code § 1798.140(d).

189. Plaintiff and Class Members seek injunctive or other equitable relief to ensure Defendant hereinafter adequately safeguards Sensitive Information by implementing reasonable security procedures and practices. Such relief is particularly important because Defendant continues to hold Sensitive Information, including Plaintiff's and Class members' Sensitive Information. Plaintiff and Class members have an interest in ensuring that their Sensitive Information is reasonably protected, and Defendant has demonstrated a pattern of failing to adequately safeguard this information.

190. Pursuant to California Civil Code § 1798.150(b), Plaintiff mailed a CCPA notice letter to Defendant's registered service agents, detailing the specific provisions of the CCPA that Defendant has violated and continues to violate. If Defendant cannot cure within 30 days—and Plaintiff believes such cure is not possible under these facts and circumstances—then Plaintiff intends to promptly amend this Complaint to seek statutory damages as permitted by the CCPA.

191. As described herein, an actual controversy has arisen and now exists as to whether Defendant implemented and maintained reasonable security procedures and practices appropriate to the nature of the information so as to protect the personal information under the CCPA.

192. A judicial determination of this issue is necessary and appropriate at this time under the circumstances to prevent further data breaches by Defendant.

PRAYER FOR RELIEF

Plaintiff and the Class demand a jury trial on all claims so triable and request that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiff and the proposed Class, appointing Plaintiff as class representative, and appointing her counsel to represent the Class;

B. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiff and the Class;

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

C. Awarding injunctive relief as is necessary to protect the interests of Plaintiff and the Class;

D. Enjoining Defendant from further deceptive practices and making untrue statements Plaintiff the Data Breach and the stolen Sensitive Information;

E. Awarding Plaintiff and the Class damages that include applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

F. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;

G. Awarding attorneys' fees and costs, as allowed by law;

H. Awarding prejudgment and post-judgment interest, as provided by law;

I. Granting Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and

J. Granting such other or further relief as may be appropriate under the circumstances.

JURY DEMAND

Plaintiff hereby demands that this matter be tried before a jury.

Dated: April 16, 2025

Respectfully submitted,

By: /s/ *Samuel J. Strauss*

Samuel J. Strauss, WSBA #46971
STRAUSS BORRELLI PLLC
One Magnificent Mile
980 N. Michigan Avenue, Suite 1610
Chicago, IL 60611
Telephone: (872) 263-1100
Facsimile: (872) 263-1109
sam@straussborrelli.com

Attorneys for Plaintiff and the Proposed Class